

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-320578

(43)Date of publication of application : 16.11.2001

(51)Int.Cl. H04N 1/387
G06T 1/00
G09C 1/00
G09C 5/00
H04L 9/08
H04N 7/08
H04N 7/081

(21)Application number : 2000-139833

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 12.05.2000

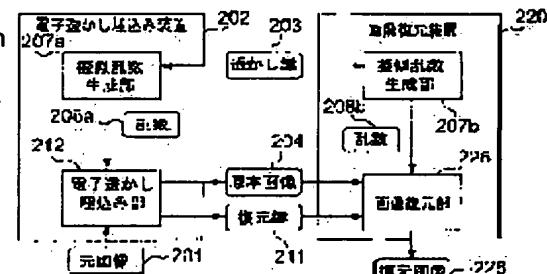
(72)Inventor : MITSUI YASUHIRO

(54) EMBEDDING METHOD VERIFYING METHOD AND RESTORING METHOD FOR ELECTRONIC WATERMARK

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic watermark embedding method capable of restoring an original image.

SOLUTION: A random number (208a) is generated (207a) by using a watermark key (203), the original real image (204) is prepared by embedding watermark information in the data of the original image (201) in an order designated by the random number, and a restoration key (211) including the data of the original image before the embedding of the watermark information (209) is generated. The original image is restored by using the original real image (204) generated in this way, the restoration key (211) and the watermark key (203). The original image (201) can be restored from the original real image (204) by utilizing the restoration key generated at the time of performing embedding in this way.



LEGAL STATUS

[Date of request for examination] 02.02.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

[of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(2)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-320578
(P2001-320578A)

(43) 公開日 平成13年11月16日 (2001.11.16)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコト [*] (参考)
H 04 N 1/387		H 04 N 1/387	5 B 0 5 7
G 06 T 1/00	5 0 0	G 06 T 1/00	5 0 0 B 5 C 0 6 3
G 09 C 1/00	6 1 0	G 09 C 1/00	6 1 0 Z 5 C 0 7 6
	5/00		5/00 5 J 1 0 4
H 04 L 9/08		H 04 L 9/00	6 0 1 E

審査請求 未請求 請求項の数20 OL (全 13 頁) 最終頁に続く

(21) 出願番号 特願2000-139833(P2000-139833)

(22) 出願日 平成12年5月12日 (2000.5.12)

(71) 出願人 000000295
沖電気工業株式会社
東京都港区虎ノ門1丁目7番12号

(72) 発明者 三井 靖博
東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

(74) 代理人 100083840
弁理士 前田 実

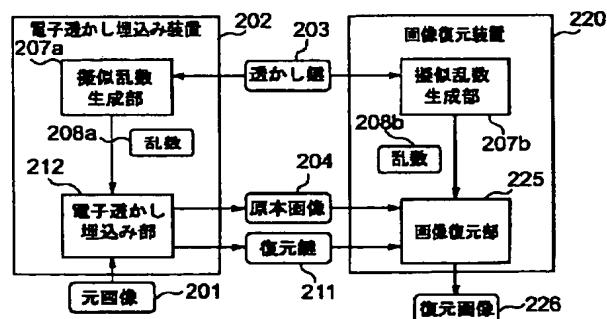
最終頁に続く

(54) 【発明の名称】 電子透かし埋込み方法、検証方法及び復元方法

(57) 【要約】

【課題】 元画像の復元が可能な電子透かし埋込み方法を提供する。

【解決手段】 透かし鍵 (203) を用いて乱数 (208a) を発生し (207a)、元画像 (201) のデータに、乱数により指定される順に、透かし情報を埋め込んで原本画像 (204) を作成し、透かし情報 (209) を埋め込む前の元画像のデータを含む復元鍵 (211) を生成する。このようにして生成された原本画像 (204) と、復元鍵 (211) と、透かし鍵 (203) とを用いて元画像を復元する。このように埋込み時に生成された復元鍵を利用することで、原本画像 (204) から元画像 (201) を復元することができる。



【特許請求の範囲】

【請求項1】 透かし鍵を用いて乱数を発生するステップと、

上記乱数により指定される元画像のデータに、上記乱数により指定される順に、透かし情報を埋め込んで原本画像を作成するステップと、

透かし情報を埋め込む前の元画像のデータを含む復元鍵を生成するステップとを含む電子透かし埋込み方法。

【請求項2】 請求項1に記載された上記原本画像と、上記復元鍵と、上記透かし鍵とを用いて元画像を復元するステップとをさらに含む元画像復元方法。

【請求項3】 上記復元鍵として、上記元画像のデータとともに、これに対応する原本画像のデータを含むものを生成することを特徴とする請求項1に記載の電子透かし埋込み方法。

【請求項4】 請求項3に記載された上記原本画像及び上記復元鍵と、請求項1に記載された上記透かし鍵とを用いて元画像を復元するステップとをさらに含み、上記復元鍵のうちの原本画像のデータと、上記原本画像の対応するデータとを照合する（互いに一致するかどうかを検証する）ことにより、原本画像及び復元鍵がともに正当のものであるかどうか（原本画像又は復元鍵が改竄されていないかどうか）を検証するステップをさらに含むことを特徴とする元画像復元方法。

【請求項5】 上記復元鍵として、上記元画像のデータとともに、上記原本画像のハッシュ値を含むものを生成することを特徴とする請求項1に記載の電子透かし埋込み方法。

【請求項6】 請求項5に記載された方法で生成された上記原本画像及び上記復元鍵と、請求項3に記載された上記透かし鍵とを用いて元画像を復元するステップと、復元の際、原本画像からハッシュ値を生成するステップとをさらに含み、

上記復元鍵に含まれるハッシュ値と、復元の際に生成したハッシュ値とを照合することにより、

原本画像及び復元鍵がともに正当のものであるかどうか（原本画像又は復元鍵が改竄されていないかどうか）を検証するステップをさらに含むことを特徴とする元画像復元方法。

【請求項7】 上記復元鍵を構成するデータを乱数により順序を変更するステップをさらに含むことを特徴とする請求項1に記載の透かし埋込み方法。

【請求項8】 上記復元鍵のデータの順序を変更するために利用する乱数が、上記透かし情報の埋込みのために利用される乱数と同じものであることを特徴とする請求項7に記載の透かし埋込み方法。

【請求項9】 請求項7又は8に記載の方法でデータの順序が変更された復元鍵を用いて原本画像から復元画像を生成することを特徴とする復元方法。

【請求項10】 請求項9に記載された、データの順序

が変更された復元鍵を、上記順序の変更に際用いられた乱数と同じ乱数を用いて順序を戻し、元の復元鍵を復元し、該復元された復元鍵を用いて原本画像から復元画像を生成することを特徴とする復元方法。

【請求項11】 元画像をビットプレーン拡張するステップと、

透かし鍵を用いて乱数を発生するステップと、上記乱数により指定される上記ビット拡張した元画像の画素の値に、上記乱数により指定される順に、透かし情報を埋め込んで原本画像を作成するステップと透かし情報を埋め込む前の元画像の画素の値を含む復元鍵を生成するステップとを含む電子透かし埋込み方法。

【請求項12】 上記ビットプレーン拡張は、復元情報を含むビットプレーンの生成を含むことを特徴とする請求項11に記載の電子透かし埋込み方法。

【請求項13】 請求項11又は12に記載された方法で生成された上記原本画像と、請求項11に記載された透かし鍵とを用いて元画像を復元するステップとをさらに含む元画像復元方法。

【請求項14】 上記復元情報を含むビットプレーンに、透かし鍵を用いて発生した乱数を用いて電子透かしを埋め込むことを特徴とする特徴とする請求項12に記載の電子透かし埋込み方法。

【請求項15】 請求項14に記載のように電子透かしを埋め込まれた復元情報を含むビットプレーンを、同じ透かし鍵を用いて発生した乱数を用いて検証を行うことを特徴とする検証方法。

【請求項16】 請求項14に記載のように電子透かしを埋め込まれた復元情報を含むビットプレーンを用いて元画像を復元することを特徴とする復元方法。

【請求項17】 元画像の各画素の値と、ビットプレーン拡張された画像の対応する画素の値が等価な関係にあり、かつビットプレーン拡張された画像の各画素の値から一意的に元画像の対応する画素の値が決まることを特徴とする請求項11に記載の埋込み方法。

【請求項18】 請求項17に記載のようにして形成されたビットプレーン拡張された生成された上記原本画像と、請求項11に記載された透かし鍵とを用いて元画像を復元するステップとをさらに含み、

上記復元の際、ビットプレーン拡張された画像の各画素の値から元画像の対応する画素の値を求める特徴とする元画像復元方法。

【請求項19】 ビットプレーン拡張された元画像の各画素の値と、透かし埋込み後の原本画像の対応する画素の値との対応関係を、一枚の画像の処理の途中で変更することを特徴とする請求項11又は17に記載の電子透かし埋込み方法。

【請求項20】 電子透かしを用いて埋め込む値と透かしを埋め込まれることにより形成される原本画像の各画素の値の対応関係を一枚の画像の処理の途中で変更する

請求項17又は19に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は画像に対する電子透かし方法に関するものである。

【0002】

【従来の技術】電子透かし技術は、例えば日経エレクトロニクス1997.2.24 (no. 683) に述べられているように、「著作権保護」の為に適用することが提案されており、画像品質を損なわないように、そして埋め込んだ透かしができるだけ消えないようにする方法が数多く提案されてきた。

【0003】一方、改竄防止の電子透かしとしては、ハッシュ情報や、特開平10-208026に述べられるようにスタンピング情報を元画像に埋込み、その情報を抽出し、比較することによって、改竄を検出するという技術が提案されている。

【0004】電子透かしの埋込みまたは検出の際に用いられる電子透かし鍵は、一般に電子透かしを秘密裏に埋め込む為のパターンを生成するために用いられている。つまり電子透かしから擬似乱数を生成し、それをを利用して埋め込むデータや詰め込む画素の選び方を複雑にすることによって、わかりにくくしている。

【0005】図23に従来構成を示し、図24に電子透かしの基本方法を示す。図23において、元画像101は電子透かしの埋込みの対象となる画像である。電子透かし埋込み装置102は透かし鍵103を基に擬似乱数生成部107aで乱数108aを生成し、電子透かし埋込み部112は乱数108aを用いて電子透かしを埋込み(120)、原本画像104を生成し、出力する。

【0006】電子透かし検証装置105では、透かし鍵103を基に擬似乱数生成部107bで乱数108bを生成し、電子透かし検証部115は乱数108bを用いて原本画像104から電子透かしを抽出し(122)、抽出された電子透かしを検証し、検証結果106を出力する。

【0007】図24において、元画像101及び原本画像104は画素の集合として表現している。各矩形部分がそれぞれ1つの画素であり中に画素番号を記述している。矩形部分がハッチングされているか否かで、その画素の色を示している。ハッチングを施した矩形部分が黒色であり画素値は「1」、ハッチングされていない矩形部分が白色で画素値は「0」である。透かし情報109は埋め込む情報を「1」または「0」の2値で示し、矩形部分のハッチングの有無は画素の色を示している。乱数108a、108bは画素番号をランダムに並べたものである。

【0008】電子透かしを埋め込む際には、乱数108aを用いて透かし情報109を元画像101に埋め込む。乱数108aで示される画素番号の最初の値は②で

あり、透かし情報109の最初の値は「1」である。そのため、元画像101の画素②の画素値を「1」に置き換える。乱数108aの次の値は④であり、透かし情報109の次の値は「0」であるため、元画像101の画素④の画素値を「0」に置き換える。この結果原本画像104ができる。

【0009】電子透かしを抽出する際には、埋込み時と同じ乱数108b(埋込み時と同じ透かし鍵103を基にして生成された乱数)を用いて透かし情報110を原本画像104から抽出する。乱数108bの最初の値は②であり、原本画像104の画素番号②の画素値は「1」であるため、透かし情報110の最初の値として「1」が抽出される。乱数203の次の値は④であり、原本画像104の画素番号④の画素値は「0」であるため、透かし情報110の次の値として「0」が抽出される。これによって抽出された透かし情報110は埋め込んだ透かし情報109と同じ値となる。

【0010】これまでの電子透かしの適用において、電子透かしの埋込みは、除去を考えて構成されたものではなかった。また除去が可能というのも、せいぜい対象画像とは別に画像全体の元画像との差分情報を保持しておき、それを用いて電子透かし埋込み済み画像から電子透かしを除去するものであった。

【0011】元々電子透かしは、人間の視覚的に影響がないように考えられており、視覚的にはそれほど変化があるわけではない。しかしながら、元画像に対しては必ず変化が起きているわけであり、明らかに元画像とは異なる。また、医療用画像などのように、元画像でないと利用できないような画像もあり、それらに対しての電子透かしの適用は、コンピュータセキュリティシンポジウム”98論文集 (IPSJ Symposium Series Vol.98 No.12) 「EZWビットストリームを用いたROI(注目領域: region of interests) 医用画像に適した電子透かし方式 (pp.57-62)」のようにROIと呼ばれる重要な部分には電子透かしを埋め込まず、その周りにのみ埋め込むといった方法をとっていた。

【0012】

【発明が解決しようとする課題】以上のように、従来、元画像を復元することができる好ましい電子透かし埋込み方法が知られていなかった。

【0013】本発明の目的は、元画像を復元することができる電子透かし埋込み方法を提供することにある。

【0014】本発明の他の目的は、復元鍵の偽造が困難な電子透かし埋込み方法を提供することにある。

【0015】本発明のさらに他の目的は、電子透かしを埋め込んだ画像と、その画像を復元するための復元情報を一つの画像として構成することができる電子透かし埋込み方法を提供することにある。

【0016】

【課題を解決するための手段】本発明の電子透かし埋め

込み方法は、透かし鍵を用いて乱数を発生するステップと、元画像のデータに、上記乱数により指定される順に、透かし情報を埋め込んで原本画像を作成するステップと、透かし情報を埋め込む前の元画像のデータを含む復元鍵を生成するステップとを含む。

【0017】

【発明の実施の形態】図1、図2、図3、及び図4はこの発明の実施の形態1を示す。図1は電子透かしの埋込み及び検証を行うための構成を示す。図の構成は、図23に示す従来の構成と同様であるが、従来技術と異なり、電子透かし埋込み装置202の電子透かし埋込み部212から復元鍵211を出力する。

【0018】図2は電子透かし埋込みと復元鍵生成の方法を示す図である。復元鍵211は透かし情報209と同じく「1」または「0」の2値で示し、矩形部分内のハッチングの有無は「1」ならば黒色、「0」ならば白色で示している。

【0019】図1及び図2に示す構成で、従来と同様な電子透かしの埋込み及び検証を行う場合には、各装置およびその構成部分の動作は従来の構成とほとんど同じである。異なるのは、本発明では画像を復元する為の鍵となる復元鍵211を出力することである。

【0020】図1及び図2において、元画像201は電子透かしの埋込みの対象となる画像である。電子透かし埋込み装置202は透かし鍵203を基に擬似乱数生成部207aで乱数208aを生成し、電子透かし埋込み部212は乱数208aを用いて電子透かしを埋込み(219)、原本画像204を生成し、出力する。

【0021】電子透かし検証装置205では、透かし鍵203を基に擬似乱数生成部207bで乱数208bを生成し、電子透かし検証部215は乱数208bを用いて原本画像204から電子透かしを抽出し、抽出された電子透かしを検証し、検証結果206を出力する。

【0022】電子透かし埋込み装置202は、上記のように電子透かしを埋め込む際に電子透かし埋込み部212において復元鍵211を生成し、出力する。復元鍵211は透かし情報209によって置き換えられた元画像201の画素値である。つまり電子透かしを埋め込む際に、まず元画像201の画素番号②の画素値「0」が最初の透かし情報「1」で置き換えられるため、復元鍵211の最初の値は「0」であり、次に元画像201の画素番号④の画素値「1」が2番目の透かし情報「0」で置き換えられるため、復元鍵211の2番目の値は「1」となる。

【0023】図3は電子透かし埋込み及び画像復元を行う際の構成であり、図4は原本画像204、乱数208b及び復元鍵211から復元画像226を生成する方法を示す。図3に示す画像復元装置220は、図1の電子透かし検証装置205と同様の擬似乱数生成部207bを備えるほか、擬似乱数生成部207bと画像を復元す

る画像復元部225を備える。擬似乱数生成部207bは透かし鍵203を基に埋込み時と同じ乱数208bを生成する。画像復元部225は、擬似乱数生成部207bで生成された乱数208bを入力とし、さらに電子透かし埋込み装置202から出力された原本画像204と復元鍵211を入力として、画像を復元し(221)、復元された画像である復元画像226を出力する。

【0024】図4に示すように、画像の復元の動作は、埋込み時と逆である。つまり乱数208bで示される画素番号の最初の値は②であり、復元鍵211の最初の値は「0」である。そのため、原本画像204の画素②の画素値を「0」に置き換える。乱数208bの次の値は④であり、復元鍵211の次の値は「1」であるため、原本画像204の画素④の画素値を「1」に置き換える。この結果復元画像226ができる、これは図2で示した元画像201と同じ画像である。

【0025】以上のように、実施の形態1によれば、電子透かし埋込み時に変更した部分の画素値から復元鍵を生成し、必要な時に復元鍵を用いて電子透かしを埋め込んだ画像から元の画像を復元することができる。

【0026】ここで作成される復元鍵の情報量は位置情報などを含まず、埋め込まれた透かし情報(即ち、変更された画素情報)と同じ量であり、復元に必要な最小情報量である。差分情報と比較しても、差分情報は画像と同じ大きさとして保持されるか、位置情報と画素情報の集合として保持されるため、絶対的に少なくなる。また処理の増加は画素値の置換だけである。

【0027】また復元鍵の値は乱数を基にランダムに並べられている為、乱数生成方法が分からなければ、原本画像と復元鍵から元画像を生成することは困難である。

【0028】図2及び図4で示す埋込み及び復元方法では、復元鍵をすり替えられた場合に検出する手段がないため、一般的な暗号手法と共に使うのが望ましい。例えば、システムとして復元鍵は基本的に移動させないで、特定の復元装置だけで必要な時に復元を行う場合は、復元鍵を暗号化し電子署名をつけてその装置内に保存し、復元したい原本画像があれば、それを復元装置に送り署名確認及び復号化を行った後復元することができるし、復元装置も分散させ復元鍵を原本画像と共に移動させる場合は、復元鍵と原本画像と一緒にアーカイブして(まとめて圧縮して)暗号化したり、相互に電子署名をつけるといった手法を取ることができる。

【0029】図5及び図6で示す埋込み及び復元方法(実施の形態2)のように、原本画像の情報を復元鍵に含めることによって復元鍵の検証を行うことができる。

【0030】図5において、復元鍵231は透かし情報209を画像に埋め込む(222)ことによって変化した画素の埋込み後と埋込み前の画素値から構成される。まず画素番号②の埋込み後画素値「1」と埋込み前画素値「0」であり、次に画素番号④の埋込み後画素値

「0」と埋込み前画素値「1」である。

【0031】図6に復元時の動作を示す。不正な偽造復元鍵234が供給された場合、復元(223)に際し、まず画素番号②の画素に対して偽造復元鍵234の埋込み後画素値は「1」であり、原本画像204の値も「1」であるため照合が成立し、偽造復元234で示される埋込み前画素値「0」に置き換えられる。次に画素番号④の画素に対して偽造復元鍵234の埋込み画素値は「1」であるが、原本画像204の画素値は「0」である。よってこの時点で復元鍵234と原本画像204が一致しないことが検出できる。システム的に復元鍵が改竄されていないことが保証できる場合は、「原本画像が改竄されているか否かどうか」という検証にもなりうる。

【0032】上記のように埋込み画素値と原本画像の画素値の不一致が検出されたときは、復元画像(226)は生成されないが、不一致が検出されないときは、復元画像が生成される。

【0033】この実施の形態2は復元鍵のサイズは実施の形態1と比べて2倍に増えているが、処理の流れとして、実施の形態1と同様に復号する為に必ずアクセスしなければならない画素だけをチェックしているため、処理としては比較処理が増えているだけであり、処理時間の増加は非常に少ない。

【0034】実施の形態2では変更画素の埋込み後画素値のみを比較する。意味のある改竄(例えば、画像中に含まれる文字を他の文字に変える変更、画像中の人物を他の人物に変える変更)を行う為には或る程度の大きさを持った改竄を行う必要があるため、大抵の場合はこの方法で問題は生じないと考えられる。

【0035】更に安全にするために、原本画像全体の情報を復元鍵に含めることもできる。図7に示す埋込み方法(実施の形態3)では、透かしを埋込む(219)ことにより生成された原本画像204全体のハッシュ値242を生成し(224)、これを復元鍵241に含めることによって原本画像204との対応を更に保証する。

【0036】即ち、このようにして透かしが埋込まれた原本画像を検証/復元する側においては、図8に示すように、乱数208bと、埋込み側から送られた復元鍵241とを用いて、原本画像204から復元画像226を得る(227)。また、原本画像204からハッシュ値243を生成し(228)、埋込み側から送られた復元鍵241内のハッシュ値242と照合する(一致するかどうか調べる:245)。そして一致していれば、原本画像204及び復元鍵241がともに改竄されていないものと判断する。一致しなければ、原本画像204及び復元鍵241の少なくとも一方が改竄されているものと判断する。原本画像204及び復元鍵241の一方について、他の方法で改竄されていないことが保証される場合には、これらの他方が改竄されているものと判断す

る。図8の検証結果247は、これらの判断の結果を表わす。

【0037】このように、実施の形態2と同様に、システム的に復元鍵が改竄されていないことが保証できる場合は、「原本画像が改竄されているか否かどうか」という検証になりうる。

【0038】なお、ハッシュ値のサイズはハッシュ関数によって固定であり、埋め込む電子透かし情報量が多い場合は、復元鍵のサイズが実施の形態2より小さくなるという利点もある。

【0039】また、実施の形態2では埋込み後の画素値のみを比較しているため、復元鍵の偽造検証として各画素の電子透かし埋込み前の値だけを変更した場合に不正が検出できない。そのため埋込み後画素値と埋込み前画素値の順番がわからないようにランダムに並べ替える方が安全である。実施の形態3においても復元鍵内におけるハッシュ値の位置が固定であると偽造し易いため同様である。

【0040】図9に示す埋込み方法(実施の形態4)では、電子透かしを元画像201に埋込んで原本画像を得るとともに(222)、電子透かし埋込み及び抽出に使う乱数208aを利用して復元鍵231をランダム化して(ランダムに並べ替えて)復元鍵251を生成する

(249)。即ち、復元鍵231のデータに最初から順番に番号付け(例では①~④)し、乱数208aでの出現順序によってデータを並び替える。図示の例では、乱数208aの最初が②のため、復元鍵251の最初の値は復元鍵231の2番目の値「0」、乱数208aの2番目の値は④のため復元鍵251の2番目の値は復元鍵231の4番目の値「1」、残る「1」と「3」のうち、乱数208aの中で次に「1」が出現する為、復元鍵251の3番目の値は復元鍵231の1番目の値である「1」、復元鍵251の最後の値は復元鍵231の3番目の値である「0」となる。この方法であれば、乱数はもともと生成されている為、復元鍵の値を並び替える処理を追加するだけで良い。

【0041】なお、復元鍵のランダム化に用いる乱数としては、埋込み位置の決定に用いる乱数とは異なるものを用いても良い。この場合には、復元鍵のランダム化に用いた乱数を発生する鍵を復元側にも与える必要がある。

【0042】図9の方法で透かしを埋込まれた原本画像を復元するには、図10に示すように、埋込み側から送られて来た復元鍵を逆ランダム化し(復元鍵のデータの順序を元に戻し:252)して元の復元鍵253を生成し、これを(乱数208bとともに)用いて、画像を復元する(254)。この場合(復元鍵を逆ランダム化する場合)、ランダム化(データの順序の変更)の逆を行う。上記の例では、復元鍵は4ビットであり、乱数の順番から、②、④、①、③と並んでいるので、その順番を

並び変える。

【0043】代りに、埋込み側から送られて来た復元鍵をそのまま（乱数208bとともに）用いて、画像を復元しても良い。この場合（逆ランダム化を行わない場合）、ランダム化（データの順序を変える）前の復元鍵とランダム化後の復元鍵の関係は、乱数（ランダム化に用いた乱数）から分かり、またランダム化前の復元鍵と復元画素値も乱数から分かる。上記の例では、最初の値は、ランダム化前の復元鍵②の値、その値はまた乱数を見て、画素④の復元画素の値であることが分かる。それ以下も、「ランダム化前の復元鍵の①の値→画素②復元画素値」、「ランダム化前の復元鍵の③の値→画素④の復元画素値」と同様に復元画素値を得る。

【0044】実施の形態1ないし実施の形態4では、元画像を復元する為の情報を復元鍵として外部に出力していたが、管理が複雑となる。以下に述べる実施の形態5ないし9は、復元鍵を生成せず、代りに画像データを拡張し復元情報を画像データ内に含めるものである。

【0045】図11及び図12に実施の形態5を示す。

【0046】図11は、電子透かし埋込み方法を示す。元画像201は1ビットのビットプレーンから成る画像（1ビット画像と呼ぶ）、拡張画像301はビットプレーン1 302、ビットプレーン0 303の2ビットのビットプレーンから成る画像（2ビット画像と呼ぶ）であり、原本画像304は、ビットプレーン0 305及びビットプレーン1 306から成るもので、拡張画像301（ビットプレーン302、303から成る）に乱数108aを用いて透かし情報109を埋め込んだ画像である。

【0047】即ち、1ビット画像である画像201は2ビット画像である拡張画像301（ビットプレーン302、303から成る）に拡張される（261）。この例では拡張は元画像201をビットプレーン1 302とし、ビットプレーン0 303の値はすべて「0」とした。

【0048】電子透かしの埋込み（263）はビットプレーン1 302に対して、先に述べた実施の形態、例えば図2の実施の形態と同様に埋込みが行われ、その結果原本画像のビットプレーン1 305が生成される。それと共に透かし情報が埋め込まれた画素（例では画素番号②と④の画素）の埋込み前画素値を原本画像のビットプレーン0 306に保持することによって、原本画像305、306を生成する。

【0049】図12は、電子透かし抽出および画像復元方法を示す。原本画像304（ビットプレーン305、306から成る）は電子透かしが埋め込まれ、かつ復元情報を持っている。透かし情報319は電子透かし抽出によって抽出された情報である。復元画像307のうちビットプレーン1 308は復元された画像である（ビットプレーン0 309は復元後不要であるので、必ず

しも生成されるものではないが、生成可能であることを示すため図示している）。

【0050】図12において、電子透かしの抽出（265）は原本画像のビットプレーン1 305から従来と同様の抽出方法で行うことができる。画像復元（265）は電子透かし抽出と共に行われ、電子透かし抽出を行った画素のプレーン0 309の画素値をプレーン1 305の画素値にコピーする。その結果生成されたビットプレーン1 308が復元された復元画像であり、これは図11に示す元画像201と同一である（同一となるはずのものである）。

【0051】以上のように、実施の形態5によれば、電子透かしを埋め込んだ画像とその画像を元画像に復元する為の復元情報を1つの画像として構成することができる。

【0052】この方法において復元情報は原本画像のビットプレーン0にしか含まれておらず、またこのプレーンの変更に対する検証がないため、このプレーンに復元情報が含まれていることがわかると復元情報の偽造が可能であり、またプレーン1に埋め込まれた電子透かしの解析もわかりやすくなってしまう。このため、改竄検出を行える電子透かしを、復元情報を含むビットプレーンに適用する方法（実施の形態6）を図13及び図14に示す。

【0053】図13において、拡張画像301（プレーン1 302及びプレーン0 303から成る）は、図11に示すものと同じである。拡張画像301のプレーン1 302に対する電子透かし209の埋込み（267）も図11の透かし埋込み263と同様である。但し、プレーン1 302への透かし埋込み前の画素値を復元情報として保持するビットプレーン0 313（図11のプレーン0 306と同じ）は中間画像311を構成するものとして、これにさらに、透かしを埋め込む（269）ことによって、原本画像314の第0のプレーン316を生成する。原本画像314のプレーン1 315は、図11のプレーン1 305と同じものである。

【0054】プレーン0 313に対する透かしの埋込みに当たっては、プレーン1 302に対する透かし埋込み（267）で使用したのと同じ乱数208aのうち、上記透かし埋込み（267）で使っていない画素番号に対応するものを使用する。それによって、プレーン0 313に含まれた復元情報を壊さないで透かし情報329を埋め込むことができる。この例では乱数の1番目（値：②）と2番目の値（値：④）はプレーン1に電子透かしを埋め込むために使用しているため、プレーン0への電子透かしは3番目（値：⑨）と4番目（値①）で示される画素に透かし情報329を埋め込む。その結果、プレーン0 313の画素番号⑨の画素値は、透かし情報329の1番目の値「0」で、画素番号①の画素

値は、透かし情報329の2番目の値「1」で置き換えられ、原本画像のプレーン0 316が生成できる。

【0055】復元時には、図14に示すように、まずプレーン0の透かし情報(329)を抽出し(270)、その値を検証することによって、改竄検出可能な電子透かしを検証し、改竄されていないことを確認し(271)、その後プレーン0の復元情報をプレーン1に適用することによって画像の復元を行う(273)ことができる。

【0056】プレーン0に改竄検出可能な電子透かしを埋め込むことによって、プレーン0の改竄を検出することができ、また復元情報しか含まれていなかったプレーン0に新たな電子透かしの情報が入り画像の複雑度が増し、プレーン1へ埋め込んだ電子透かしへの攻撃が難しくなる。

【0057】上記の実施の形態5及び実施の形態6並びに後述の実施の形態7はビットプレーン拡張可能な画像であれば適用可能である。ビットマップフォーマットとして良く知られたBMP/DIB(device independent bitmap)形式としては、1ビット、4ビット、8ビット、16ビット、24ビット、32ビットがある。また基本的に電子透かしは1つの画素に1ビット若しくは3ビット(RGB毎に1ビット)程度しか埋め込むことはないため、

1ビット画像→(1+1)ビット必要→4ビット画像
4ビット画像→(4+1)ビット必要→8ビット画像
8ビット画像→(8+1)ビット必要→16ビット画像
16ビット画像→(16+3)又は(16+1)ビット必要→24または32ビット画像
24ビット画像→(24+3)又は(24+1)ビット必要→32ビット画像

に拡張して適用できる。

【0058】ビットプレーン拡張の方法として、実施の形態5で示したように単純に0または1に値が固定されたプレーンを追加することが一番簡単である。しかしながら、ビットプレーンが複数ある画像を拡張する場合、固定値のプレーンを追加するだけでは元画像との色の違いが大きくなる。そのためその場合は画素値を考慮したビットプレーン拡張を行う必要がある。

【0059】図15に2ビットのビットプレーンを持つ元画像の値のプレーン拡張を例として示すが、単純にプレーン追加では最適な画素値にならないため、画素値が最適な値になるように(即ち、元画像の各画素の値と拡張画像の対応する画素の値とが等価な関係となるように)画素値を決めることによって元画像と等価に見える拡張画像を作ることができる。

【0060】上記方法で生成した最適な拡張画像は単純プレーン追加の場合と異なり、ほとんどの場合使っていないプレーンが無い。そのため電子透かし埋込み方法も変える必要がある。

【0061】図16に最適な拡張を行った拡張画像に電子透かしを埋め込む値の割当て例を示す。埋め込む際に埋め込んだ値と元の画素値が分かる(埋込み後の値から元の画素値を一意的に決めることができる)画素値にすることで、電子透かしを埋込み、かつ画像を復元することができる。

【0062】図16の値割当て例を用いた電子透かし埋込み(411)の例を実施の形態7として図17に示す。乱数403aの1番目の値が②であり透かし情報4

10 02の1番目の値が「0」であるため、画素番号②の画素に「0」を埋め込むために拡張画像404の画素番号②の画素値「0101」を「0100」に変更し、乱数403aの2番目の値が④であり透かし情報402の2番目の値が「1」あるため、画素番号④の画素に「1」を埋め込むために拡張画像404の画素番号④の画素値「1010」を「1011」に変更し、乱数403aの3番目の値が⑨であり、透かし情報402の3番目の値が「1」であるため、画素番号⑨の画素に「1」を埋め込むために拡張画像404の画素番号⑨の画素値「0000」を「0001」に変更し、乱数403aの4番目の値が⑤であり透かし情報402の4番目の値が「0」であるため、画素番号⑤の画素に「0」を埋め込むために拡張画像404の画素番号⑤の画素値「1111」を「1110」に変更することによって原本画像406を生成する。

【0063】図18に電子透かし抽出(413)及び画像復元(415)の例を示す。乱数403bの1番目の値が②であり原本画像406の画素番号②の画素値が「0100」であるため、「0」が埋め込まれていることが分かり透かし情報422の1番目の値は「0」と抽出され、画素値「0100」の元の画素値は必ず「0101」であるため「0101」に変更する。同様にすべての透かし情報を抽出し、画素値を復元することによって拡張画像424が復元できる。また、拡張画像424の各画素値から元の画像の画素値は一意的に決まるため、元画像421が復元できる。原本画像から拡張画像、また拡張画像から元画像への画素値対応はどちらも一意的であるため、拡張画像を生成しなくとも、原本画像から元画像を生成することもできる。

【0064】実施の形態7では、埋込み方法としてビットプレーン0だけを変更した埋込み値を示したが、別の埋込み値を利用することも可能である。この例の様にビットプレーンが2倍に増えた場合、取り得る画素値は4倍になっており、図19に示す例のように各画素値が重なり合わない画素値であればどの画素値でも利用することができます。図19の例では元の画素値が「0:0000」の場合、電子透かしを埋め込んだ後の画素値として、「0:0000」、「1:0001」、「2:0010」、「3:0011」の画素値のどれかを使うことができ、それらはすべて復元時に画素値「0:0000

0」に復元できる。

【0065】拡張画像の画素値と埋込み後の画素値の対応パターンが一つであると、埋込み後の画素値から拡張画像の画素値を推測して、元画像が取出される可能性がある。そのため図20に示す実施の形態8のように複数の対応パターンを準備して、処理途中で変更することによって、拡張画像の画素値を推測しにくくすることができる。対応パターンは画質劣化の許容範囲内で用意しておき、処理の順番(例えば1番目の画素はパターン0、2番目の画素はパターン1、…等によって、使用する対応パターンを変化させるわけである。

【0066】電子透かしを用いて埋め込む値の割当てを変化させる方法もある。「0」と「1」の2値を埋め込む場合、図21に示す埋込み値割当てパターン例の様に4つの対応画素値があれば、割当てパターンは $P_2 = 4! / (4-2)! = 12$ パターン存在する。その割当てパターンを処理途中で変更するわけである。

【0067】図22に図21で示した埋込み値割当てパターン例を使った実施の形態9の電子透かし埋込み例(417)を示す。ここでは処理の順番によって割当てパターンを図21の割当てパターン順番で適用している。まず乱数433の1番目の値は⑥であり画素番号⑥の画素に透かし情報432の1番目の値「0」を埋め込むために1番目の割当てパターンであるパターン0(0埋込み:0000, 1埋込み:0001)を適用する。同様に2番目の画素番号⑨の画素にはパターン1(0埋込み:0001, 1埋込み:0011)を、3番目の画素番号⑩の画素にはパターン2(0埋込み:0011, 1埋込み:0100)を適用すると、原本画像436ができる。この例を見て分かるように、拡張画像の画素値と埋め込む透かし情報の値が同じ場合でも画素値が異なる原本画像が生成される。

【0068】なお、実施の形態1ないし実施の形態4で、復元鍵をそのまま出力したが、圧縮して出力すれば更に短い復元鍵とすることができます。

【0069】実施の形態5ないし実施の形態9では、「0」「1」の2値の埋込み例を示したが、別の埋込み値を利用することも可能である。この例の様にビットプレーンが2倍に増えた場合、取り得る画素値は4倍になっており、4値まで埋め込むことが可能である。

【0070】実施の形態1ないし実施の形態4で画素の復元のために変更前画素値を復元鍵のデータとしていたが、2値の場合、復元の為の画素演算「そのまま」か「反転」のデータとすることも可能である。同様に実施の形態5(図11)でプレーン0の値も、変更前画素値でなく画素演算「そのまま」か「反転」のデータとすることができます。

【0071】

【発明の効果】本発明の実施の形態1ないし実施の形態4によれば、少量のデータ(復元鍵)を生成して送るだ

けで元画像の復元が可能となる。

【0072】本発明の実施の形態5ないし実施の形態9によれば、ビットプレーン拡張を行ったのち透かしの埋込みを行うので、復元のための情報の改竄が一層困難となる。

【0073】請求項1の方法によれば、復元鍵を生成するので、これを利用することで、原本画像から元画像を復元することができる。

【0074】請求項2の方法によれば、元画像や原本画像に比べはるかに少量のデータから成る復元鍵を伝達するのみで、元画像の復元を行うことができる。

【0075】請求項3の方法によれば、復元鍵が原本画像のデータを含むので、これと原本画像の対応するデータとを照合することにより、原本画像又は復元鍵のいずれかが改竄されていないかどうかの検証を行うことができる。

【0076】請求項4の方法によれば、元画像や原本画像に比べはるかに少量のデータを伝達するのみで、原本画像又は復元鍵の検証を行うことができる。

【0077】請求項5の方法によれば、復元鍵が原本画像のハッシュ値を含むので、これを用いて原本画像の全体又は復元鍵が改竄されていないかどうかの検証を行うことができる。しかも、原本画像の全体について上記の検証を行うことができる。

【0078】請求項6の方法によれば、元画像や原本画像に比べはるかに少量のデータを伝達するのみで、原本画像の全体又は復元鍵の検証を行うことができる。

【0079】請求項7の方法によれば、復元鍵を構成するデータを乱数により並べ替えるので、復元鍵の偽造が一層困難とである。

【0080】請求項8の方法によれば、復元鍵の並べ替えに用いられた乱数を発生するための鍵を別途伝達する必要がない。

【0081】請求項10の方法によれば、復元鍵を構成するデータを乱数により並べ替えるので、復元鍵の偽造が一層困難である。

【0082】請求項11の方法によれば、電子透かしを埋め込んだ画像と、その画像を復元するための復元情報を1つの画像として構成することができる。

【0083】請求項14の方法によれば、復元情報の偽造が困難である。

【0084】請求項17の方法によれば、原本画像と元の画像との類似性が色に関し、一層高くなる。

【0085】請求項19の方法には、拡張画像と埋込み後の画像との対応関係が変化するので、埋込み画像の画素の値から拡張画像の画素の値を推測するのが困難だという効果がある。

【0086】請求項20の方法には、拡張画像の画素の値の推測が困難だと言う効果がある。

【図面の簡単な説明】

【図1】 本発明の実施の形態1の透かし埋込み及び検証のための装置の一例を示すブロック図である。

【図2】 実施の形態1における透かし埋込み方法を示す概略図である。

【図3】 本発明の実施の形態1の透かし埋込み及び復元のための装置の一例を示すブロック図である。

【図4】 実施の形態1における透かし復元方法を示す概略図である。

【図5】 本発明の実施の形態2の透かし埋込み及び復元のための装置の一例を示すブロック図である。

【図6】 実施の形態2における透かし復元方法を示す概略図である。

【図7】 実施の形態3における透かし埋込みを示す概略図である。

【図8】 実施の形態3における透かし検証／復元を示す概略図である。

【図9】 実施の形態4における透かし埋込みを示す概略図である。

【図10】 実施の形態4における透かし検証／復元を示す概略図である。

【図11】 本発明の実施の形態5の透かし埋込み方法を示す概略図である。

【図12】 実施の形態5の透かし復元を示す概略図である。

【図13】 実施の形態6の透かし埋込みを示す概略図である。

【図14】 実施の形態6の透かし検証／復元を示す概略図である。

* 【図15】 実施の形態7におけるプレーン拡張の例を示す概略図である。

【図16】 実施の形態7における、透かし埋込み前後の各プレーンのデータを示す図である。

【図17】 実施の形態7における、透かし埋込みの例を示す図である。

【図18】 実施の形態7における、電子透かし抽出及び画像復元の例を示す図である。

【図19】 実施の形態7における、埋込み値の異なる例を示す図である。

【図20】 実施の形態8における、拡張画像の画素値と埋込み後の画素値の対応パターンの関係を示す図である。

【図21】 実施の形態9における、電子透かしを用いて埋め込む値の割当てを変化させる方法の一例を示す図である。

【図22】 図21で示した埋め込み値割当てパターン例を使った実施の形態9の電子透かし埋込み例を示す。

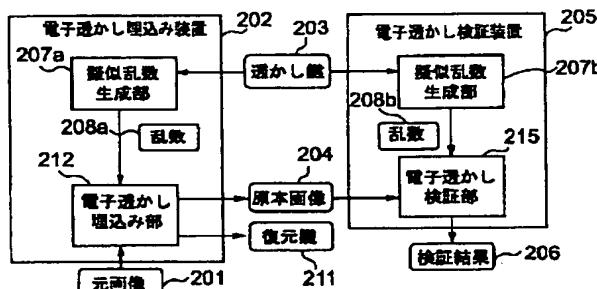
【図23】 従来の透かし埋込み及び検証を行う装置の一例を示すブロック図である。

【図24】 従来の装置における透かし埋込み及び電子透かしの抽出の方法を示す概略図である。

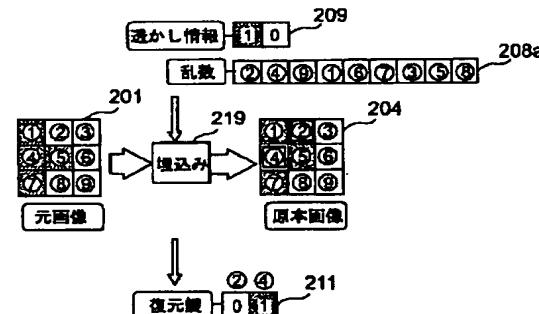
【符号の説明】

202 電子透かし埋込み装置、 205 電子透かし検証装置、 207a、 207b 擬似乱数生成部、 212 電子透かし埋込み部、 215 電子透かし検証部、 220 画像復元装置、 225 画像復元部。

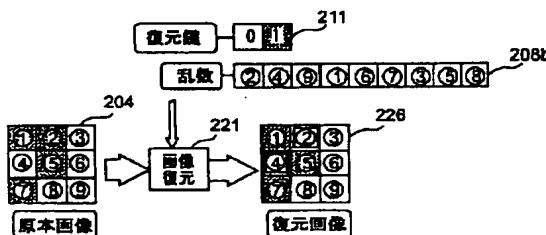
【図1】



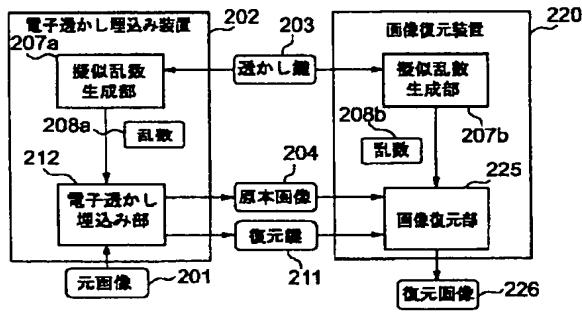
【図2】



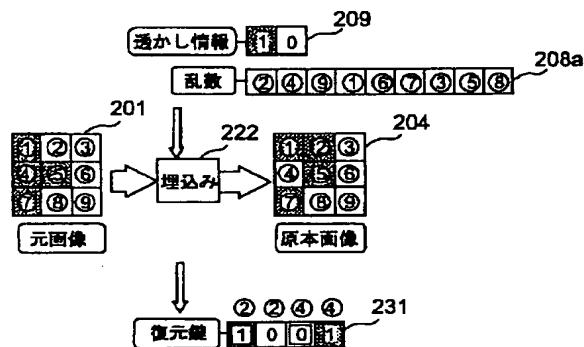
【図4】



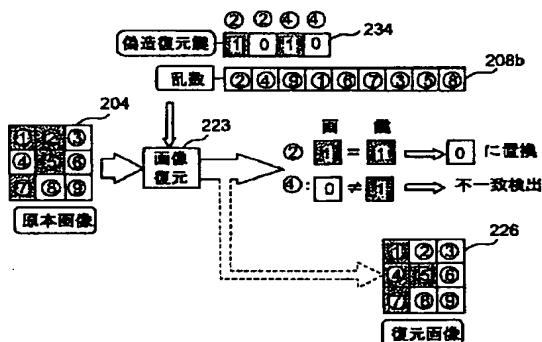
【図3】



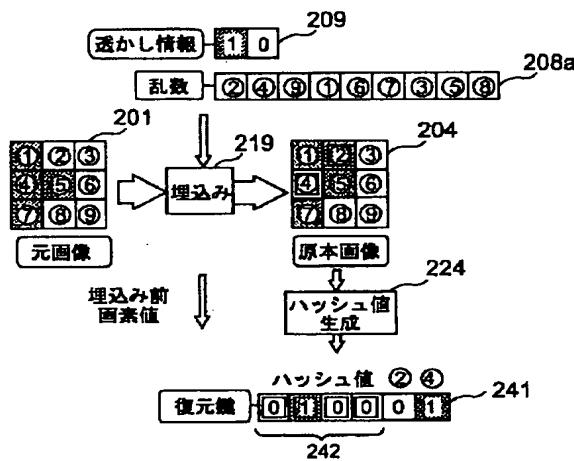
【図5】



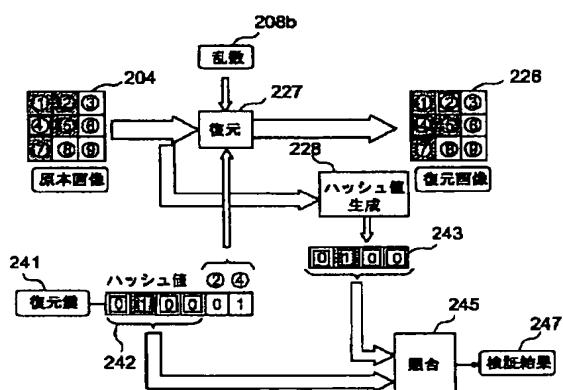
【図6】



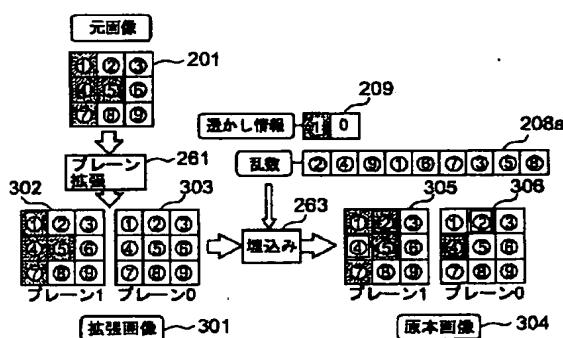
【図7】



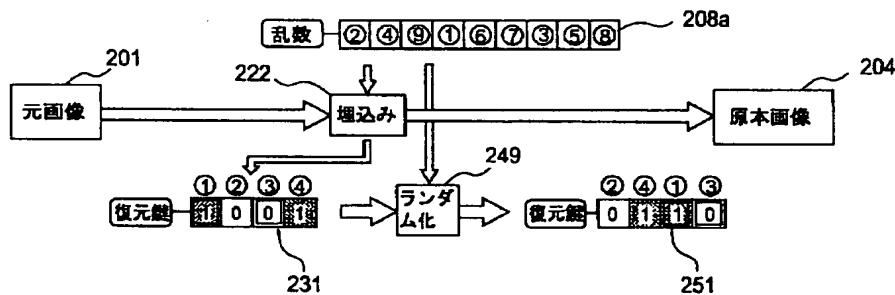
【図8】



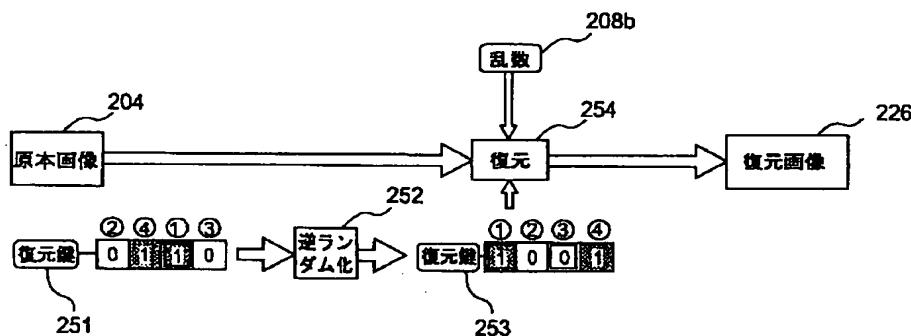
【図11】



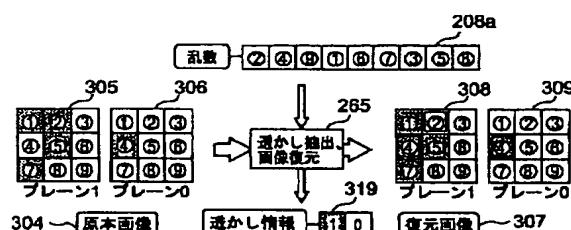
【図9】



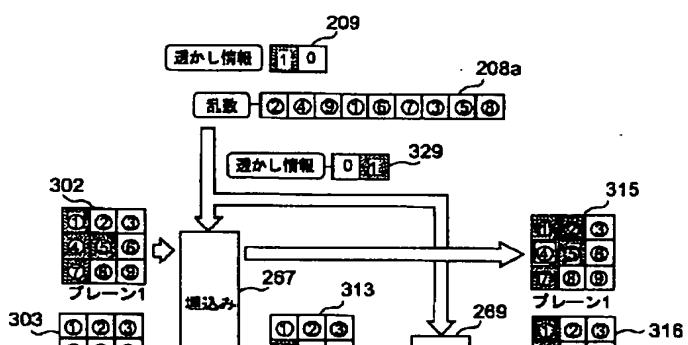
【図10】



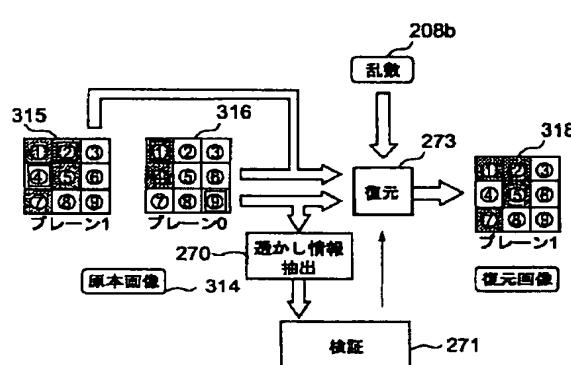
【図12】



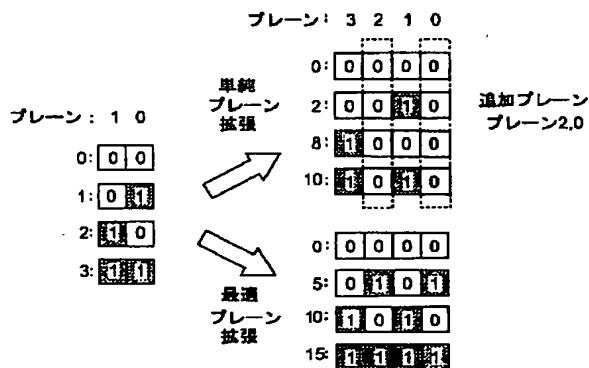
【図13】



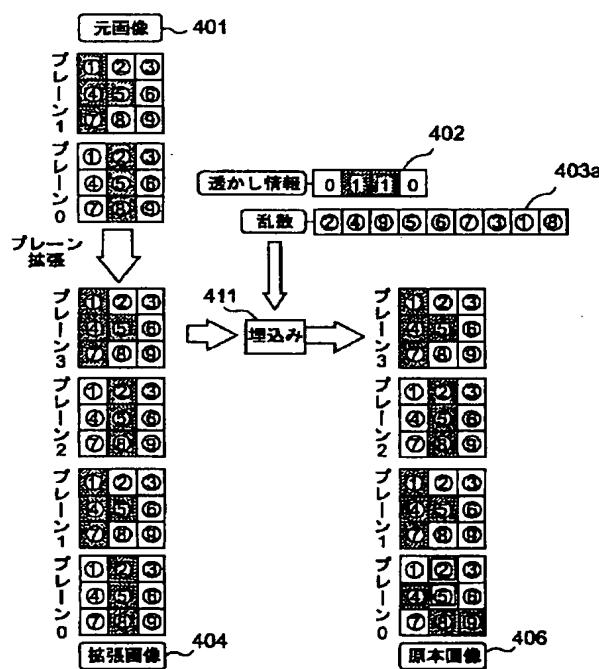
【図14】



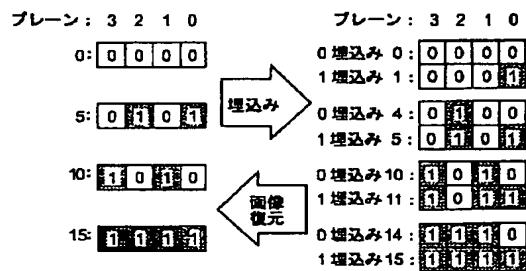
【図15】



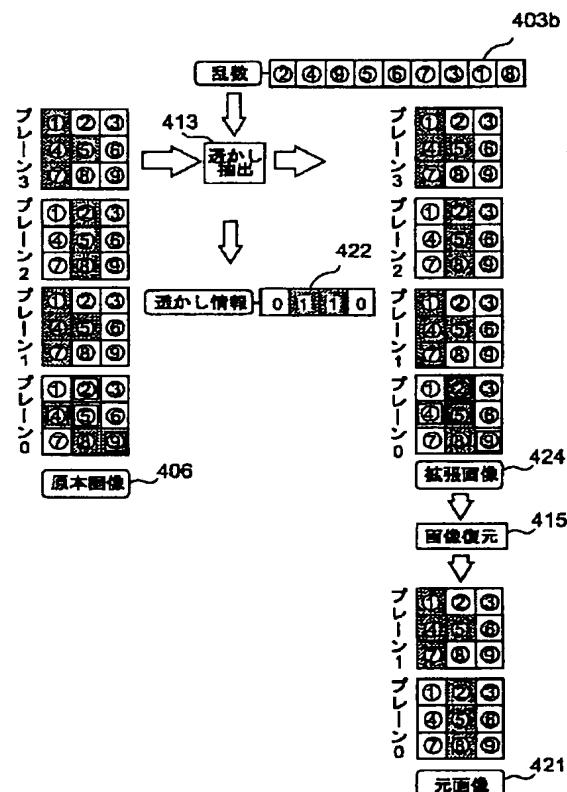
【図17】



【図16】



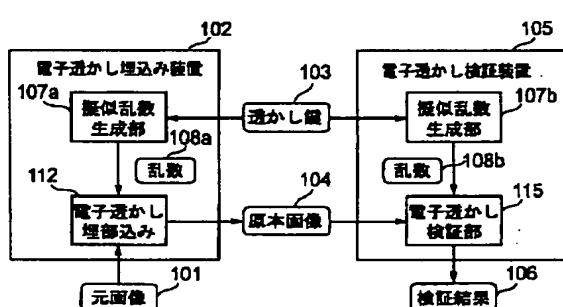
【図18】



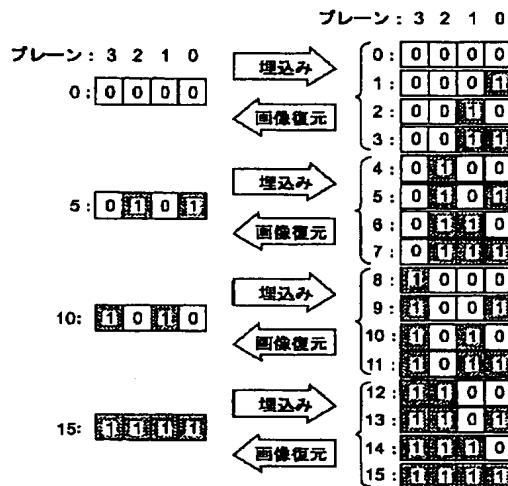
【図21】

フレーン	埋込み値割当てパターン															
	3	2	1	0	0	1	2	3	4	5	6	7	8	9	10	11
0:	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1
1:	0	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1
3:	0	0	1	1	1	0	0	1	1	1	0	1	1	0	1	1
4:	0	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0

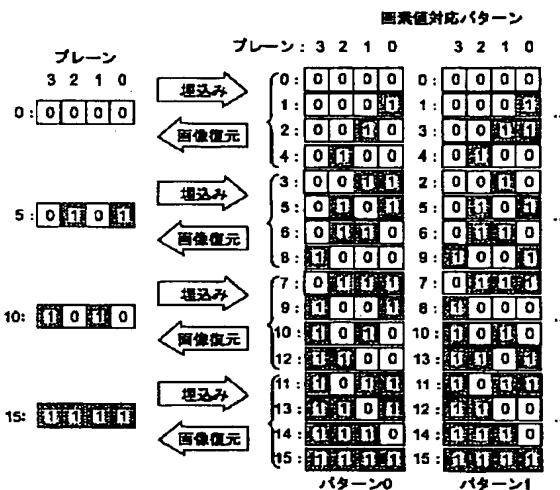
【図23】



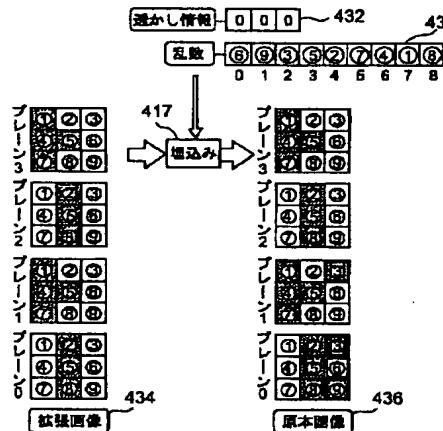
【図19】



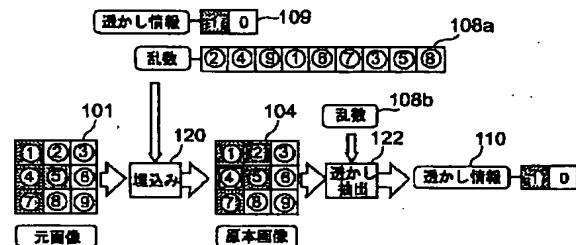
【図20】



【図22】



【図24】



フロントページの続き

(51) Int. Cl.

H 0 4 N 7/08
7/081

識別記号

F I

H 0 4 L 9/00
H 0 4 N 7/08

「マーク」(参考)

6 0 1 A
Z

F ターム(参考) 5B057 CA12 CA16 CB12 CB16 CB19
CC03 CE08 CE09 CG07 CH08
CH18 DA07 DA08 DA17
5C063 AB03 AB05 AC02 AC10 CA34
CA36 DA13
5C076 AA01 AA14 BA06 CA10
5J104 AA01 AA08 AA14 AA16 EA04
EA17 JA03 LA02 NA02 NA12